

EKOKEM PÄÄKONTTORIN WLAN



Ammattikorkeakoulun opinnäytetyö

Tietotekniikan ko.

Riihimäen yksikkö, 17.10.2011

Sami Länsimaa

Tietotekniikan koulutusohjelma
Riihimäki

Työn nimi Ekokem pääkonttorin WLAN

Tekijä Sami Länsimaa

Ohjaava opettaja Raimo Hälinen

Hyväksytty _____._____.2011

Hyväksyjä

Riihimäki
Tietotekniikan ko.
Tietoliikenne

Tekijä	Sami Länsimaa	Vuosi 2011
Työn nimi	Ekokem pääkonttorin WLAN	

TIIVISTELMÄ

Tämän opinnäytetyön tarkoitus oli selvittää millaisia langattoman lähiverkon ratkaisuja ja palveluita laitetoimittajilla on tarjota työn toimeksiantajan Ekokem Oy Ab:n pääkonttorille Riihimäkeen.

Työssä sovellettu teoria koostui tunnettujen laitevalmistajien ja standardeista vastaavien järjestöjen dokumentoinneista koskien langattomia lähiverkko- ja 4. sukupolven (4G) mobiiliverkkotekniikoita. Työssä tutustuttiin laajasti nykyaikaisiin 802.11g/n Wireless Local Area Network (WLAN)-standardeihin, sekä mobiiliverkkojen Long Term Evolution (LTE)- ja Worldwide Interoperability for Microwave Access (WiMAX)-tekniikoiden perusteisiin. Teoriatiedon lisäksi työssä hyödynnettiin 2010 Ekokemillä suoritettua WLAN-kartoitusta.

Kerättyjen taustatietojen perusteella määriteltiin Ekokemin tarpeet täyttävä WLAN-verkko ja määritelmään perustuvat tarjouspyynnöt lähetettiin viidelle eri tietoliikennealan yritykselle. Raportti sisältää yhteenvedon jokaisesta tarjouksesta, sekä suositukset varteenotettavavimmasta tarjouksesta.

Valmis raportti antaa toimeksiantajalle selkeän kuvan nykyaikaisista WLAN- ja 4G-tekniikoista, sekä siitä millaisella laiteratkaisulla suunniteltu WLAN-verkko voitaisiin tulevaisuudessa toteuttaa.

Avainsanat WLAN, 802.11, 802.1X, WiMAX, LTE

Sivut 27 s, + liitteet 6 s.

Riihimäki
Degree Programme in Information Technology
Telecommunication

Author	Sami Länsimaa	Year 2011
Subject of Bachelor's thesis	Ekokem's head office WLAN	

ABSTRACT

The purpose of this thesis was to find out what kinds of wireless local area network solutions and services can suppliers offer for the thesis commissioner Ekokem Oy Ab's head office in Riihimäki.

The theory that was applied in this research consisted of documentation from known manufacturers and organizations responsible for standards of wireless local area networks and 4. generation (4G) mobile network technologies. Modern 802.11g/n Wireless Local Area Network (WLAN) standards were widely explored and also an overview of mobile network technologies such as Long Term Evolution (LTE) and Worldwide Interoperability for Microwave Access (WiMAX) was made. Besides the theoretical knowledge, this research also took advantage of a WLAN survey that had been performed at Ekokem in 2010.

Based on the gathered background information, a WLAN network that met Ekokem's needs was defined. Then offer requests, based on these definitions were sent to five different companies working in the field of telecommunications. The thesis contains a summary of every offer that was made, and recommendations on the most viable offer.

This finalized report will give a clear picture to the commissioner of modern WLAN and 4G technologies and also how the defined Ekokem WLAN network could be executed in the future.

Keywords WLAN, 802.11, 802.1X, WiMAX, LTE

Pages 27 p + appendices 6 p.

SISÄLLYS

1	JOHDANTO.....	1
1.1	Ekokem Oy Ab.....	2
2	NYKYAIKAISET WLAN-STANDARDIT	3
2.1	Langattoman tiedonsiirron käsitteitä.....	3
2.2	802.11g.....	4
2.2.1	Modulaatio ja siirtonopeudet.....	4
2.2.2	Kanavat.....	5
2.3	802.11n.....	6
2.3.1	Multiple-Input Multiple-Output	6
2.3.2	Taajuudet ja kanavat.....	6
2.3.3	Toimintatilat	7
3	LANGATON LAAJAKAISTA NYT JA TULEVAISUUDESSA	8
3.1	Worldwide Interoperability for Microwave Access.....	8
3.1.1	Modulaatio, taajuudet ja kanavat.....	8
3.1.2	Tiedonsiirtonopeudet ja päätelaitteet.....	9
3.2	Long Term Evolution	9
3.2.1	Modulaatio, taajuudet ja kanavat.....	10
3.2.2	Tiedonsiirtonopeudet ja päätelaitteet.....	10
3.3	Mobiilitiedonsiirron tulevaisuus	11
3.3.1	Worldwide Interoperability for Microwave Access 2.....	11
3.3.2	Long Term Evolution-Advanced.....	11
3.3.3	Käyttöönotto	11
4	SALAUS JA AUTENTIKOINTI.....	12
4.1	Wi-Fi Protected Access.....	12
4.2	Wi-Fi Protected Access 2.....	13
4.3	802.1X.....	13
5	EKOKEM PÄÄKONTTORIN LANGATON VERKKORATKAISU.....	15
5.1	WLAN-verkon määrittely	15
5.2	Daimler Finlandin tarjous.....	16
5.3	Nylund Group tarjous.....	17
5.4	Elisan tarjous	18
5.5	AinaCom tarjous	19
5.6	LAN&WAN Nordic tarjous	20
5.7	Suosituksset	21
6	YHTEENVETO	23
	LÄHTEET	24
Liite 1	WLAN-VERKON KUVAUS	

1 JOHDANTO

WLAN eli langaton lähiverkko on nykyaikainen, joskaan ei kovin uusi keksintö tietoliikennetekniikassa. Kuluttajamarkkinoille suunnattua WLAN-tekniikkaa on ollut tarjolla jo vuodesta 1999. Vaikka kyseistä tekniikkaa on ollut jo hyvän aikaa tarjolla, on sen hyödyntäminen ollut näihin päiviin asti kovin vähäistä varsinkin yritysverkkojen osalta. Alkuaikoina leviämistä jarruttivat laitteiden korkea hinta ja lisäksi vanhoilla WLAN-standardeilla ei kyetty kilpailemaan tiedonsiirtonopeuksissa ja tietoturvasa langallisen verkon kanssa.

Uusien WLAN-standardien myötä tiedonsiirtonopeudet ovat moninkertaistuneet ja ne kykenevät jo tarjoamaan täysin varteenotettavan vaihtoehdon langalliselle verkolle. Toinen merkittävä ja vakavasti otettava seikka on tietoturva. Tietoturvaa on myös uusilla standardeilla tehostettu merkittävästi ja näin saavutetaan lähes yhtä turvallinen toimintaympäristö kuin langallisella verkolla.

Tässä opinnäytetyössä tullaan keskittymään kahteen uusimpaan langattoman lähiverkon standardiin, joita ovat 802.11g ja 802.11n. Toimeksiantajan eli Ekokem Oy Ab yrityksen toivomuksesta langattomien lähiverkkojen lisäksi tehdään myös lyhyt katsaus langattomista laajakaistatekniikoista. Näihin tekniikoihin kuuluvat nykyaikaiset WiMAX- ja LTE-standardit, sekä näiden kehitysaskeleet WiMAX2 ja LTE-Advanced.

Opinnäytetyön tavoitteina on tutkia nykyaikaisia WLAN-standardeja ja määritellä teorialiedon, sekä 2010 suoritettun kartoituksen pohjalta Ekokemin tarpeisiin soveltuva WLAN-verkko. Määrittelyn perusteella pyydetään viideltä yritykseltä tarjoukset heidän tarjoamistaan palveluista ja laiteratkaisuista. Lopuksi raporttiin kirjataan kunkin tarjouksen pääkohdat ja omat suositukseni Ekokemin tarpeita parhaiten palvelevasta tarjouksesta. Valmis raportti tulee toimimaan neuvoa-antavana dokumenttina WLAN-verkon hankintaa koskevia päätöksiä tehtäessä.

1.1 Ekokem Oy Ab

Opinnäytetyöni toimeksiantaja Ekokem-konsernin emoyhtiö Ekokem Oy Ab:n päätoimipaikka sijaitsee Riihimäellä. Lisäksi on lukuisia sivutoimipisteitä, jotka sijaitsevat Kouvolassa, Iisalmessa, Joensuussa, Jämsänkoskella, Kuopiossa, Porissa, Oulussa, Turussa, Ylivieskassa ja Seinäjoella. Ekokem-konserniin kuuluu emoyhtiön lisäksi Ekokem-Palvelu Oy ja Ekovoima Oy.

Ekokem Oy Ab tarjoaa kattavat ympäristöhuoltopalvelut yrityksille, yhteisöille ja kunnille eri puolilla Suomea. Ekokem Oy Ab:n liiketoiminta perustuu ongelma- ja teollisuusjätteiden hyödyntämiseen, vaarattomaksi tekemiseen ja loppusijoittamiseen. Yhtiön perustamisesta lähtien 1979 on toiminnan päämääränä ollut Suomen ympäristösuojelun edistäminen.

Ekokem-konserni työllisti vuoden 2010 lopulla yhteensä 315 työntekijää. Konsernin tunnusluvuihin mainittakoon vuoden 2010 liikevaihto 110 M€, liikevoitto 15,7 M€ ja omavaraisuusaste 69,1 %.



Kuva 1 Ekokem Oy Ab Riihimäen toimipiste

2 NYKYAIKAISET WLAN-STANDARDIT

WLAN eli langaton lähiverkko on nykyaikana sen verran laajalle levinnyttä tekniikka, että varmasti jokainen tietokoneiden kanssa tekemisissä oleva on tähän tekniikkaan törmännyt. Ennen kuin siirrytään tarkemmin tarkastelemaan nykyaikaisia WLAN-standardeja, on syytä selvittää muutamia langattomaan tekniikkaan liittyviä käsitteitä.

WLAN-standardit ovat Institute of Electrical and Electronics Engineers (IEEE):n eli kansainvälisen tekniikan alan järjestön laatimia. WLAN-verkkoja määrittelevät standardit ovat hyvin teknisiä dokumentteja, jotka sisältävät tarkat tiedot uudesta tekniikasta. Standardeihin tutustuminen ja niiden ymmärtäminen vaativat lukijaltaan: tiedonsiirtotekniikan, modulaatiotekniikan ja radiotekniikan perusteiden ymmärrystä. Tässä dokumentissa on tarkoituksella jätetty pois sellaisia teknisiä yksityiskohtia, joilla ei ole katsottu olevan suurta merkitystä toiminnallisuuden ymmärtämisen suhteen.

2.1 Langattoman tiedonsiirron käsitteitä

WLAN-verkon voidaan ajatella koostuvan suppeimmillaan kahdesta laitteesta, jotka lähettävät toisilleen tietoa langattomasti radiotiellä. WLAN-verkon peruslaitteena toimii WLAN-tukiasema, johon päätelaite kuten kannettavatietokone tai esimerkiksi nykyaikainen älypuhelin on yhteydessä langattomasti. Näiden laitteiden välinen tiedonsiirto sitten perustuu johonkin WLAN-standardiin. Kun sekä tukiasema, että päätelaite molemmat tukevat samaa standardia, niin tiedonsiirtäminen radiotiellä langattomasti on mahdollista. Tukiasemalta eteenpäin tiedonsiirto voi sitten jatkua sekä radiotiellä, että langallista verkkoyhteyttä pitkin.

WLAN-standardit taas määrittelevät laitteille ja langattomalle tiedonsiirrolle yhteiset pelisäännöt. Näihin määritelmiin lukeutuvat radiotiellä käytettävät kanavat, jotka ovat taajuusalueilla 2,4 Gigahertsiä (GHz) ja/tai 5 GHz. Näiden taajuusalueiden vapaa käyttö perustuu kansainvälisiin sopimuksiin. Kanavasta voidaan ajatella samaan tapaan kuin eri radiokanavilla on eri taajuudet esimerkiksi NRJ 97,3 Megahertsiä (MHz) tai Radio Nova 100,2 MHz, niin myös tiedonsiirrossa on omat määrätyt kanavansa joilla laitteet toimivat.

Standardit määrittelevät myös käytettävän modulaatiotavan ja tällä taas tarkoitetaan keinoa, jolla siirrettävä tieto saadaan liitettyä kanavan taajuuteen. Uusimpia langattomia tekniikoita käsiteltäessä tämä modulaatiotapa on Orthogonal Frequency-Division Multiplexing (OFDM)-menetelmä tai siihen pohjautuvat Orthogonal Frequency-Division Multiple Access (OFDMA) ja Single-Carrier FDMA (SC-FDMA). OFDM-menetelmän peruseriaate on jakaa kanava alikanaviin ja lähettää tieto radiotiellä näitä alikanavia pitkin samanaikaisesti. Sama peruseriaate on käytössä OFDMA- ja SC-FDMA-menetelmissä, joita käytetään nykyaikaisissa WiMAX- ja LTE-verkoissa.

Yksi käyttäjän kannalta mielenkiintoisimmista käsitteistä on tiedonsiirtonopeus, joka nykyisissä tekniikoissa vaihtelee hitaimmillaan 6 Megabitistä sekunnissa (Mbps) aina jopa 600 Mbps nopeuksiin. On kuitenkin huomiotavaa, että eri tekniikoiden yhteydessä puhuttavilla maksimi tiedonsiirtonopeuksilla tarkoitetaan nimenomaan radiotiellä siirtyvän tiedon maksiminopeuksia, joka sisältää käyttäjän lähettämän tiedon lisäksi huomattavasti ohjaukseen ja virheenkorjaukseen tarvittavaa tietoa. Näin ollen todelliset hyötytiedon eli hyötykuorman siirtonopeudet ovat esimerkiksi 802.11g-standardilla noin 25 Mbps eli alle puolet radiotiellä tapahtuvasta tiedonsiirrosta maksiminopeudella 54Mbps. Lisäksi on myös hyvä tiedostaa, että siirtonopeus jakautuu vielä kaikkien tukiasemaan liittyvien käyttäjien kesken.

2.2 802.11g

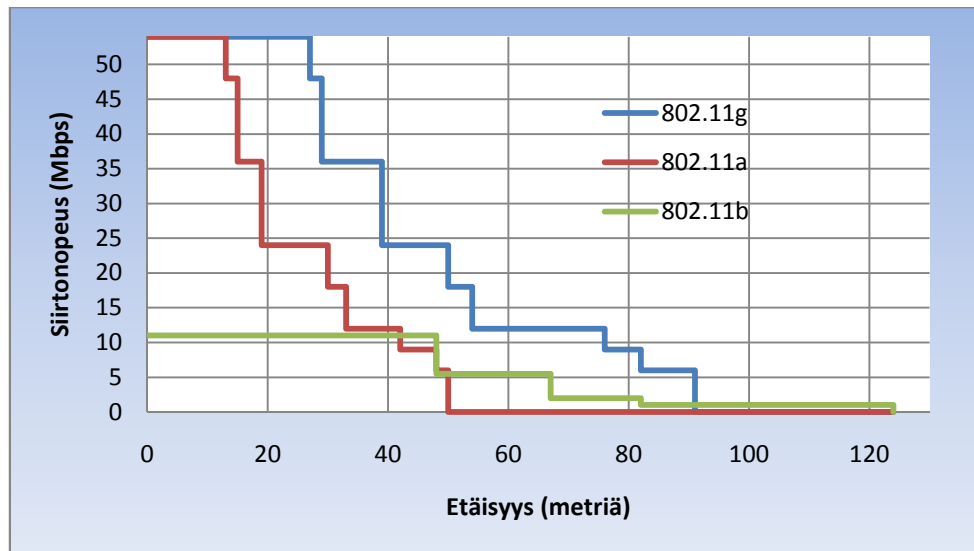
IEEE 802.11g on vuonna 2003 julkaistu standardi, joka mahdollistaa maksimi tiedonsiirtonopeuden 54 Mbps. Tämä standardi kehitettiin korvaamaan 1999 julkaistu 802.11b, jonka tiedonsiirtonopeus ylsi maksimissaan 11 Mbps. Toinen mainitsemisen arvoinen edeltäjä on 2001 julkaistu 802.11a, joka ylsi jo tuolloin 54Mbps nopeuksiin. 802.11a ei kuitenkaan menestynyt, koska se ei ole yhteensopiva vanhojen 802.11b-tuotteiden kanssa. Tekniikka ei ole yhteensopivaa, koska se toimi korkeammalla taajuusalueella 5 GHz ja käytti erilaista modulaatiomenetelmää. (IEEE 802.11g 2003, 2-3.)

802.11g otettiin julkaisunsa jälkeen hyvin tehokkaasti käyttöön ja suurimpana syynä suosioon oli yhteensopivuus vanhojen 802.11b-laitteiden kanssa, sekä kasvanut tiedonsiirtonopeus. Nykyään vanhempia laitteita ei enää juuri käytössä näe vaan ne on vuosien saatossa saatu korvattua 802.11g- tai uusimman 802.11n-standardin laitteilla. (Cisco Systems 2005, 1.)

2.2.1 Modulaatio ja siirtonopeudet

802.11g-laitteet tukevat kahta eri modulaatiotapaa, joista vanhempi Direct Sequence Spread Spectrum (DSSS) eli suorasekvenssi hajaspektri on perua vanhasta 802.11b-tekniikasta. DSSS tuki on säilytetty vanhan 802.11b-standardin yhteensopivuuden säilymiseksi. Uudempi modulaatiotapa OFDM eli monikantaaltomodulaatio taas on tehokkaampi ja se on käytössä 802.11g-laitteiden välisessä tiedonsiirrossa.

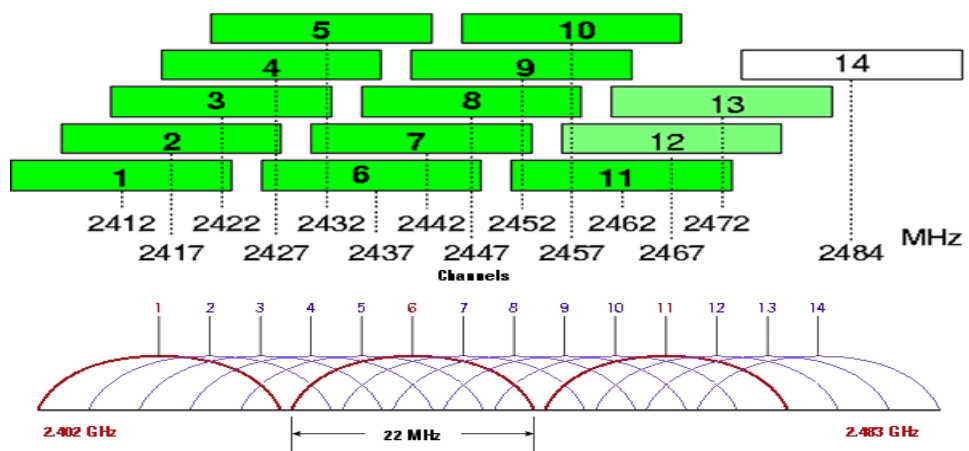
802.11-standardien laitteille on ominaista, että ne tukevat useita tiedonsiirtonopeuksia. Näin nopeutta saadaan säädettyä sen mukaan kuinka kaukana laitteet ovat toisistaan. Esteettömässä ympäristössä siirtonopeudet vaihtelevat edempänä esitetyn kuvan 2. mukaisesti. Tällä menetelmällä saadaan vähennettyä tiedonsiirrossa tapahtuvien virheiden määrä kun nopeutta lasketaan etäisyyden kasvaessa. 802.11g-laitteilla nopeudet ovat OFDM-modulaatiolla 54, 48, 36, 24, 18, 12, 9 ja 6 Mbps. Vanhalla DSSS-modulaatiolla nopeudet ovat 11, 5.5, 2 ja 1 Mbps. (IEEE 802.11g 2003, 3; Cisco Systems 2005, 1.)



Kuva 2 Siirtonopeudet

2.2.2 Kanavat

802.11g-laitteet toimivat 802.11b-standardin tapaan samalla 2,4 GHz taajuusalueella. Vuonna 1985 määriteltyä 2,4 GHz taajuuskaistaa kutsutaan Industrial, Scientific and Medical (ISM)-kaistaksi. ISM-kaista on maksuton ja vapaassa käytössä ympäri maailman. Kaista jakautuu 13 kanavaksi kuvan 3. mukaisesti siten, että 2,401–2,483 GHz taajuusalue on jaettu 20 MHz kanaviksi. Joissakin poikkeus maissa kuten Japanissa on käytössä vielä 14:sta kanava. Kanavien määrä on saatu näin suureksi limittämällä kanavat osittain päällekkäin. ISM-kaistalla on näin ollen valittavissa vain kolme toisiaan häiritsemätöntä kanavaa, joita ovat 1|6|11, 1|7|13, 2|7|12 tai 3|8|13. Kanavien limittäminen aiheuttaa vierekkäisten tukiasemien kanavavalinnan ongelmalliseksi, koska vierekkäiset kanavat häiritsevät toisiaan voimakkaasti ja taas itsenäisiä kanavia on käytössä vain 3 kappaletta. (Industrial Scientific and Medical (ISM) Bands 1993; WLAN n.d; Channels for 802.11g n.d.)



Kuva 3 ISM-kaista

2.3 802.11n

Vuonna 2009 julkaistu 802.11-standardin uusin lisäys n tuo mukanaan lukuisia parannuksia, joilla saavutetaan nopeampi tiedonsiirto ja signaalin kantama. 802.11n-standardin laitteet ovat myös yhteensopivia vanhojen 802.11b/a/g-standardien kanssa. Uusien tekniikoiden myötä siirtonopeudet ovat kasvaneet a/g-standardien 54 Mbps aina 600 Mbps. Samalla signaalin kantama on kasvanut 100 metristä peräti 150 metriin avoimessa sisätilassa. (802.11n primer 2008, 4; Paul DeBeasi 2008, 6.)

2.3.1 Multiple-Input Multiple-Output

Yksi merkittävistä uudistuksista on (MIMO)-tekniikka, joka mahdollistaa signaalin lähettämisen ja vastaanottamisen usean antennin kautta. 802.11n-standardin laitteissa antennien määrä voi vaihdella yhdestä neljään. MIMO-tekniikan avulla on mahdollista saavuttaa suurempi tiedonsiirtonopeus pilkkomalla lähetettävä tieto osiin ja lähettämällä osat eri antenneilla samanaikaisesti eli puhutaan tilallisesta limityksestä. On myös huomioitavaa, että tämä tekniikka toimii sitä paremmin mitä enemmän signaalin heijastumista tapahtuu. Tällöin laite pystyy tehokkaammin erottamaan eri antennien läheteet toisistaan. Eli avoin tila, jossa signaalit kulkevat suoraan heijastumatta esteistä ei ole MIMO-tekniikan kannalta edullisin. (802.11n primer 2008, 5.)

2.3.2 Taajuudet ja kanavat

802.11n-laitteet toimivat sekä 2,4 GHz Industrial, Scientific and Medical eli (ISM)-kaistalla, että 5 GHz Unlicensed National Information Infrastructure eli (UNII)-kaistalla. ISM-kaistalla on käytössä samat 13 20 MHz limitettyä kanavaa kuin b/g-standardeillakin, mutta UNII-kaista tarjoaa peräti 23 kappaletta 20 MHz itsenäistä kanavaa. UNII kanavien käyttö tulee vielä käytännöllisemmäksi pyrittäessä suuriin tiedonsiirtonopeuksiin, sillä 802.11n pystyy hyödyntämään 40 MHz kanavia. Näin ollen kanavia yhdistelemällä saadaan 23 kanavasta 11 40 MHz kanavaa. ISM-kaistalla kanavien yhdistely ei ole järkevää, koska itsenäisiä 20 MHz kanavia on vain 3 kappaletta ja näin ollen olisi mahdollisuus käyttää vain yhtä 40 MHz kanavaa. Leveämpi kaista tarkoittaa suurempaa tiedonsiirtonopeutta eli kun 20 MHz kanavassa saadaan siirtymään 72,2 Mbps niin 40 MHz kanavassa saadaan siirrettyä 150 Mbps. Näistä saadaan muodostettua 802.11n-standardin teoreettinen maksimi tiedonsiirtonopeus siten, että käytössä on 40 MHz kanava ja 4 antennia eli 150 Mbps kertaa 4 on 600 Mbps. Radiotiellä tapahtuvan tiedonsiirron lisäksi on muistettava ottaa myös huomioon tukiaseman liityntä lankaverkkoon. On varmistettava, että lankaverkon kapasiteetti riittää myös palvelemaan saavutettuja nopeuksia. Vanha 100 Mbps langallinen verkko saattaa aiheuttaa pullonkaulan yhdistettynä tukiasemaan, joka kykenee yli 100Mbps tiedonsiirtonopeuksiin. (802.11n primer 2008, 6-7; Paul DeBeasi 2008, 8; Connect 802 n.d.)

2.3.3 Toimintatilat

802.11n-standardin laitteilla on kolme toimintatilaa: High Throughput eli (HT), Non-HT ja HT Mixed. Näiden toimintatilojen avulla voidaan helposti määrittää yhteensopivuus mahdollisiin verkossa vielä liikennöiviin vanhemman standardin laitteisiin. HT-tilassa laite toimii pelkästään uuden standardin mukaisesti ja tätä tilaa käytetään silloin kun verkossa ei ole vanhaan standardiin perustuvia tukiasemia tai päätelaitteita.

Non-HT-tilassa laite taas toimii pelkästään vanhojen standardien mukaisesti ja tällöin kaikki tieto lähetetään 802.11a/g-standardien edellyttämässä muodossa. Tässä tilassa ei saavuteta 802.11n-standardin suorituskykyä eli tiedonsiirtonopeudet ovat maksimissaan 54 Mbps.

HT Mixed taas on yleisimmin käytettävä toimintatila ja sen avulla säilytetään vanhojen laitteiden yhteensopivuus ja samalla saadaan käyttöön osa uuden standardin eduista. Tässä tilassa yhteensopivuuden säilyttämiseksi joudutaan tekemään kompromisseja, joten n-standardin laitteet eivät pääse aivan maksiminopeuksiinsa. (802.11n primer 2008, 10-11.)

3 LANGATON LAAJAKAISTA NYT JA TULEVAISUUDESSA

Ekokemin työntekijät hyödyntävät tällä hetkellä toimistolta poissa ollessaan third generation (3G) eli kolmannen sukupolven mobiileja tiedonsiirtoyhteyksiä saadakseen yhteyden yrityksen verkkoresursseihin. Tästä syystä esittelen työssäni myös langattomia laajakaistaratkaisuja. Tarve nopeaan ja langattomaan tiedonsiirtoon riippumatta ajasta ja paikasta on kiihdyttänyt uusien standardien kehitystä ja nyt toiminnassa olevien 3G-verkkojen seuraava kehitys askel eli fourth generation (4G)-tekniikat tekevät tuloaan. Yleisesti neljännen sukupolven verkoista puhuttaessa törmätään sellaisiin kilpaileviin standardeihin kuin Long Term Evolution (LTE) ja Worldwide Interoperability for Microwave Access (WiMAX). WiMAX sinänsä ei ole uusi standardi vaan se on ollut olemassa jo vuodesta 2003 markkinoilla tarjoten kiinteitä langattomia laajakaistaratkaisuja. Kuitenkin vasta viimeisimmät standardin kehitysaskleet tekevät siitä 4G:n nopeaan tiedonsiirtoon soveltuvan standardin. Toisin kuin WiMAX niin LTE taas on uutta tekniikkaa, joka on puhtaasti suunniteltu seuraavaksi kehitysaskeliksi matkapuhelinverkon nopeaan tiedonsiirtoon.

Vaikka näillä näkymin seuraavaksi mobiiliverkkojen 4G-tekniikaksi on suurten puhelinoperaattoreiden myötävaikutuksesta jo käytännössä varmistunut LTE, niin ei WiMAX ole suinkaan huonompi tai käytöstä poistunut. WiMAX-tekniikalla toteutettuja langattomia laajakaistaverkkoja on tämän hetkisen tiedon mukaan käytössä ja suunnitteilla yhteensä 583 kappaletta ympäri maailman ja lisää on tulossa. Eli WiMAX on jo valmista ja testattua tekniikka. LTE taas on sen verran uusi tulokas, että Suomessakin on käytössä vasta muutamia testiverkkoja. (Prossori 2011.)

3.1 Worldwide Interoperability for Microwave Access

WiMAX-tekniikka perustuu saman IEEE järjestön määrittelemiін standardeihin kuin aiemmin käsitellyt WLAN-standardit. Ensimmäinen WiMAX-standardi eli 802.16a valmistui 2003 ja sillä kyettiin jo lyhyen etäisyyden kiinteisiin langattomiin laajakaista yhteyksiin. Standardilla saavutetut yhteydet olivat niin sanottuja näköyhteydellisiä yhteyksiä eli tukiaseman ja vastaanottimen välillä ei saanut olla merkittäviä näköesteitä. 2004 julkaistu laajennus eli 802.16REVd mahdollisti asiakaspäätelaitteen sijoittamisen sisätiloihin eli näköyhteys ei ollut enää välttämätön. 2005 julkaistu 802.16e-standardi sitten mahdollisti myös liikkuvien päätelaitteiden käytämisen. (Alcatel n.d 1-2.)

3.1.1 Modulaatio, taajuudet ja kanavat

WiMAX hyödyntää WLAN-standardeistakin tuttuun OFDM-modulaatioon pohjautuvaa OFDMA-menetelmää siirtäessään tietoa kanavassa molempiin suuntiin tukiaseman ja asiakaspäätteiden välillä. Langattomista lähiverkoista poiketen WiMAX-standardeille on määritelty hyvin laaja taajuusalue ulottuen 2 GHz:sta jopa 66 GHz taajuuksiin.

Käytännön toteutuksissa on kuitenkin pääasiassa hyödynnetty 2,5 GHz ja 3,5 GHz taajuuksia, koska ne ovat monissa maissa vielä vapaina olevia taajuuksia. Lisäksi matalampi taajuus kantaa pidemmälle ja esteiden läpäisykyky on parempi kuin korkeilla taajuuksilla. Kanavat taas jakautuvat siten, että valitulla taajuusalueella voidaan käyttää 1.25, 2.5, 5, 10 tai 20 MHz kanavia. Myös WLAN-standardeista tuttu MIMO, jossa sekä lähettykseen että vastaanottoon käytetään samanaikaisesti useampaa kuin yhtä antennia on WiMAX-tekniikalle määritetty. (Mobile WiMAX n.d, 8-9; Tejas Bhandare. 2008, 18.)

3.1.2 Tiedonsiirtonopeudet ja päätelaitteet

On huomioitavaa, että WiMAX kuten muillakin langattomilla tekniikoilla siirtonopeus radiotiellä on aina monen tekijän summa. Tiedonsiirtonopeuteen keskeisesti vaikuttavia tekijöitä ovat:

- Kanavan kaistanleveys (1.25–20 MHz)
- OFDMA kantaaltojen modulaatiotapa (Binary phase-shift keying (BPSK), Quadrature phase-shift keying (QPSK), Quadrature amplitude modulation (QAM))
- Hyötykuorman määrä suhteessa virheenkorjaus tietoon ($\frac{1}{2}$, $\frac{2}{3}$, $\frac{3}{4}$)
- Lähettävien ja vastaanottavien antennien määrä (1-4)
- Etäisyys tukiasemasta (0 → 15km)
- Tukiasemaan kytkeytyneiden tilaajien määrä.

Yllä mainittujen tekijöiden summana siirtonopeus on mahdollista määrittää tarpeen ja vallitsevien olosuhteiden mukaan väliltä 1-75 Mbps. Esimerkkinä käytännön toteutuksesta tekniikalla on mahdollista saavuttaa 10 Mbps siirtonopeus 10 km päähän tukiasemasta.

WiMAX-asiakaspätelaitteet ovat samankaltaisia ja helppokäyttöisiä, kuin nykyiset DSL tai kaapelimodeemit. Kannettaviin tietokoneisiin voidaan kytkeä WiMAX-kortti esimerkiksi USB-väylään. Pitkät etäisyydet tukiasemaan vaativat ulkoisen antennin käyttöä. (Mobile WiMAX n.d, 10; Alcatel n.d 3; Tejas Bhandare. 2008, 5.)

3.2 Long Term Evolution

Mobiiliverkkojen tiedonsiirto standardeista vastaava 3rd Generation Partnership Project (3GPP)-järjestö aloitti LTE-tekniikan kehitystyön vuonna 2004. LTE on seuraava kehitysaskel nykyisille kolmannen sukupolven High-Speed Downlink Packet Access (HSDPA) ja High-Speed Uplink Packet Access (HSUPA)-tekniikoille. Uuden standardin tavoitteiksi on asetettu 3-4 kertainen latausnopeus verkosta asiakaspätelaitteelle ja 2-3 kertainen latausnopeus asiakaspätelaitteelta verkon suuntaan verrattuna 3G-tekniikoihin. Hetkelliset maksiminopeudet olisivat 100 Mbps tukiasemalta päätelaitteelle ja 50 Mbps toiseen suuntaan 20 MHz kanavalla käytettäessä MIMO-tekniikkaa. (WiMAX forum 2009, 20.)

3.2.1 Modulaatio, taajuuudet ja kanavat

LTE hyödyntää WiMAX tekniikasta poiketen kahta modulaatiomenetelmää siten, että tukiasemalta päätelaitteelle käytössä on OFDMA-menetelmä ja toiseen suuntaan SC-FDMA. SC-FDMA-modulaatiolla saavutetaan päätelaitteelle pienempi virrankulutus, mikä on mobiililaitteiden akkukeston kannalta tärkeää. LTE-tekniikassa käytetään jo olemassa olevien mobiiliverkkojen taajuuksia eli 800 MHz, 900 MHz, 1800 MHz ja 1900 MHz. Olemassa olevien verkkojen lisäksi LTE toimii myös uusilla taajuusalueilla 800 MHz - 2,62 GHz. Kanavan koko voi vaihdella samaan tapaan kuin WiMAX-tekniikassa eli 1.25, 2.5, 3, 5, 10, 20 MHz kanavat ovat käytössä. (Radio-electronics n.d; Tejas Bhandare 2008, 46.)

3.2.2 Tiedonsiirtonopeudet ja päätelaitteet

Tiedonsiirtonopeudet määräytyvät samojen tekijöiden mukaisesti kuin WiMAX-tekniikassakin eli kaistanleveys, kantoaaltojen modulaatiotapa, virheenkorjaustiedon määrä, antenni konfiguraatiot, etäisyys tukiasemaan ja verkon ruuhkaisuus ovat ratkaisevia tekijöitä. Koska LTE-verkot vasta tekevät tuloaan, niin todellisista siirtonopeuksista ei vielä ole kovinkaan paljon tutkimusmateriaalia saatavilla. Paperilla luvataan 100–326 Mbps nopeuksia verkosta asiakaspäätteelle ja 50–86 Mbps asiakkaalta verkkoon. Arviodut nopeudet tulevat käytännön kaupallisissa toteutuksissa olemaan noin 30–80 Mbps verkosta ladattaessa. TeliaSoneran pilottiverkossa on testeissä saavutettu parhaimmillaan 50 Mbps latausnopeus. Päätelaitteet tulevat olemaan 3G-tekniikasta tuttuja eli matkapuhelimiin ja kannettaviin tietokoneisiin integroitua piirejä, sekä pöytätietokoneisiin sisäänrakennettuja tai ulkoisia laajennuskortteja. LTE-asiakaspäätelaitteet tulevat jakautumaan viiteen luokkaan MIMO-tukensa ja tiedonsiirtonopeuksien mukaan. 1. luokan laitteet toimivat yhdellä antennilla ja siirtonopeudet ovat noin 10 Mbps, kun taas kalleimman 5. luokan laitteet kykenevät jopa 300 Mbps nopeuksiin. (Tietokone 2010; Prosessori 2009.)

3.3 Mobiilitiedonsiirron tulevaisuus

International Telecommunication Union (ITU) eli kansainvälinen televiestintäliitto on jo määritellyt vaatimustasot nykyisiä LTE- ja WiMAX-tekniikoita seuraaville standardeille. Maksimi latausnopeus verkosta nopeudella 10 km/h liikkuvalla käyttäjälle tulisi olla 1000 Mbps ja nopeasti 350 km/h liikkuvilla käyttäjillä 100 Mbps. Huimien latausnopeuksien lisäksi uusille standardeille on asetettu minimi vaatimuksia koskien muun muassa: käytettävää kaistanleveyttä, viiveitä ja Voice over Internet Protocol eli (VoIP) kapasiteettia. (WiMAX forum 2009 24.)

3.3.1 Worldwide Interoperability for Microwave Access 2

IEEE:n 802.16m-standardi on WiMAX:n seuraava kehitysaskel ja sen on tarkoitus täyttää tai jopa ylittää ITU:n asettamat vaatimukset. Käytettävä taajuusalue tulee olemaan alle 6 GHz, mutta käytännössä 450–3800 MHz. Latausnopeudeksi verkosta on luvattu vähintään ITU:n määrittämät 1000 Mbps hitaasti liikkuville ja 100 Mbps nopeasti liikkuville käyttäjille. Luvutut nopeudet tullaan saavuttamaan kasvattamalla kanavan kaistanleveyttä nykyisestä maksimista 20 MHz aina 40 MHz kaistanleveyksiin. Tämän lisäksi kaistanleveyttä saadaan kasvatettua yhdistelemällä kanavia, jolloin saadaan käyttöön 100 MHz kaista. Mobiilikäyttäjien tuki luvataan jopa 500 km/h liikkuville käyttäjille. Standardin lopullinen hyväksyminen tapahtui 31. Maaliskuuta 2011. Ensimmäisiä WiMAX 2 verkkoja suunnitellaan rakennettavaksi jo vuoden 2012 aikana. (WiMAX forum 2009 25-27; Networkworld 2010; IEEE Standards Association 2011.)

3.3.2 Long Term Evolution-Advanced

Alustavien tietojen perusteella 3GPP:n (LTE-A)-standardi tulee oleman hyvin samankaltainen kuin edellä esitelty WiMAX 2. Latausnopeudet 1000 Mbps mikä saavutetaan hitaasti liikkuvilla eli käytännössä jalankulkunopeuksilla. Korkeaa suorituskykyä luvataan 120 km/h nopeuksiin asti ja yhteys tukiasemaan säilyy aina 350 km/h nopeuksiin asti. Käyttöön saadaan myös 40 MHz kanavat ja kaistanleveys skaalautuu välillä 20–100 MHz. (TATA n.d 11-12.)

3.3.3 Käyttöönotto

WiMAX 2-tekniikalla on selkeä etulyönti asema verrattaessa LTE-A:han, koska se on ajallisesti noin 2-3 vuotta edellä. Nähtäväksi jää kuinka moni operaattori valitsee WiMAX 2-tekniikan seuraavan sukupolven verkkoratkaisuun. Erään ennusteen mukaan WiMAX tilaajia olisi vuoteen 2013 mennessä jo 140 miljoonaa. Eli vaikka LTE on operaattoreiden jo omaksumaa tekniikkaa niin nähtäväksi jää kuinka moni uskaltaa jäädä vuosiksi odottamaan seuraavaa versiota. (WiMAX forum 2009 29-30.)

4 SALAUS JA AUTENTIKOINTI

Radiotiellä siirrettävän tiedon salaaminen ja verkkoon liittyvien käyttäjien tunnistaminen on ollut tiedonsiirto standardien tapaan jatkuvan kehityksen alla. Vuonna 1997 julkaistu ensimmäinen WLAN-verkoille suunnattu salaus ja käyttäjien autentikointiin tarkoitettu menetelmä Wired Equivalency Privacy (WEP) oli erittäin helposti murrettavissa ja näin ollen se onkin jo käytöstä poistunut menetelmä. Heikoksi havaitun WEP-menetelmän korvaajaa suunnittelemaan perustettiin vuonna 2001 IEEE 802.11i-työryhmä. Koska paine WEP-menetelmän korvaamiseksi oli erittäin suuri, niin jo ennen 802.11i valmistumista julkaistiin vuonna 2003 Wi-Fi Protected Access (WPA). WPA sisälsi jo tulevan 802.11i-menetelmän keskeisimmät toiminnot. 802.11i eli paremmin WPA2 nimellä tunnettu menetelmä julkaistiin 2004, joka sisälsi vielä muutamia uudistuksia koskien tiedon salausta. WPA2 julkaisun jälkeen on keskitytty salauksen sijaan autentikointiin eli verkon käyttäjien ja verkonlaitteiden väliseen tunnistukseen. (Wi-Fi Alliance 2009 4-5; Airmagnet n.d 2-4.)

4.1 Wi-Fi Protected Access

WPA-menetelmä siis julkaistiin 2003 korvaamaan vanha ja tietoturva näkökulmasta heikko WEP. WEP-menetelmällä käyttäjien tunnistus suoritettiin ainoastaan yksipuolisella tunnistuksella eli verkkoon liittyvän tietokoneen tarvitsi vain lähettää tietty salasana tukiasemalle liittyäkseen verkkoon. Tukiasema ei millään tavalla todentanut itseään verkkoon liittyvälle koneelle, mikä osaltaan heikentää tietoturvaa. WEP-menetelmässä tiedon salaaminen perustuu Rivest Cipher 4 eli (RC4)-salausalgoritmiin. WEP:n heikkous ei kuitenkaan johtunut käytetystä salausalgoritmista vaan tavasta jolla algoritmia hyödynnettiin. Näihin heikkouksiin lukeutuu salausavaimen lyhyys 40 bittiä ja se, että koko verkossa käytettiin yhtä ja samaa salausavainparia kaikkien laitteiden välisessä tiedonsiirrossa. Eli näin ollen yhden avainparin murtaminen riitti koko verkon salauksen murtamiseen. (Wi-Fi Alliance 2009 5; Airmagnet n.d 2-3.)

WPA käyttää myös RC4-salausalgoritmia, mutta sen käytössä hyödynnetään Temporal Key Integrity Protocol (TKIP)-menetelmää. TKIP-menetelmässä salausavainpari vaihtuu aika-ajoin ja on siten paljon hankalampi murtaa. Käyttäjien tunnistukseen voidaan käyttää vähemmän kriittisissä ympäristöissä kuten kotiverkossa Pre Shared Key (PSK) eli ennalta jaettua avainta, jolloin verkkoon liittyessä on tiedettävä salasana jolla verkkoon liittyminen on sallittu. Yritysverkoissa käyttäjien tunnistus on järkevää suorittaa yksilöllisemmin ottamalla käyttöön jokin 802.1X-standardin tarjoamista menetelmistä. Käyttäjien autentikoinnista puhutaan tarkemmin myöhemmässä kappaleessa. (Airmagnet n.d 5; Wi-Fi Alliance 2009 5.)

4.2 Wi-Fi Protected Access 2

WPA2 eroaa WPA:sta vain salauksensa osalta eli siinä TKIP on korvattu Counter Mode with Cipher Block Chaining Message Authentication Code Protocol eli (CCMP)-menetelmällä ja RC-4 on korvattu Advanced Encryption Standard (AES)-salausalgoritmillä. AES on tällä hetkellä kaikkein varmin tiedon salaukseen käytettävä algoritmi. Toisaalta sen käyttäminen kyllä vaatii tietokoneelta enemmän laskentatehoa ja kaikkein vanhimmat koneet eivät edes tue sitä. Useimmissa langattoman verkon tukiasemissa on mahdollisuus valita yhteensopivuustila, jolloin vanhoille laitteille salaus voidaan suorittaa TKIP-menetelmällä. Autentikointi on WPA:n tavoin mahdollista toteuttaa sekä ennalta jaetulla avaimella PSK tai hyödyntämällä 802.1X-standardin menetelmiä, joista kerrotaan seuraavassa kappaleessa. (Airmagnet n.d 5.)

4.3 802.1X

802.1X on puhtaasti autentikointi menetelmiä määrittelevä standardi, jonka lukuisia verkkolaitteiden ja käyttäjien tunnistukseen suunniteltuja menetelmiä voidaan yhdistää edellä mainittuihin WPA tai WPA2:teen. Eli salauksen määrittää WPA tai WPA2, mutta autentikointi voidaan korvata jollakin 802.1X-menetelmistä. Näiden menetelmien käyttöönotto vaatii useimmiten varsinaisen WLAN-verkon laitteiden lisäksi Authentication, Authorization ja Accounting eli (AAA)-palvelimen. AAA-palvelimena käytetään tyypillisimmin Remote Authentication Dial In User Service (RADIUS)-protokollalla toimivaa palvelinta. Windows-ympäristössä RADIUS-palvelimet kulkevat vanhemmissa Windows-palvelimissa nimellä Internet Authentication Service (IAS), mutta uudemmissa IAS on korvattu Network Policy Server eli (NPS)-palvelulla.

AAA-palvelimen tarkoitus on tarjota keskitetty tietokanta jota vasten käyttäjät voidaan verkossa tunnistaa. AAA-palvelin mahdollistaa verkkoliikenteen seurannan, tilastoinnin, käyttäjäkohtaisen tunnistuksen ja käyttöoikeuksien määrittämisen. Yritysverkoissa on mahdollista hyödyntää jo olemassa olevaa esimerkiksi Windows toimialueen hallintakoneen eli Domain Controllerin Active Directory-käyttäjätietokantaa. AAA-palvelimen hankinta ei kuitenkaan ole täysin pakollista, koska autentikointitietojen kysely voidaan monissa tapauksissa suorittaa esimerkiksi Lightweight Directory Access Protocol (LDAP) avulla. LDAP on protokolla, jonka avulla voidaan suorittaa esimerkiksi käyttäjän tietojen kysely suoraan Active Directorystä. (Airmagnet n.d 3-4; Wi-Fi Alliance 2009 6-7; Cisco WLC 2009.)

802.1X-standardin palvelimet kuten edellä mainittu RADIUS hyödyntävät tunnistuksessa Extensible Authentication Protocol (EAP)-protokollaa. EAP määrittää tavan jolla käyttäjien tunnistus tulee suorittaa ja näistä suosituimpia ovat:

- Lightweight Extensible Authentication Protocol (LEAP) (2 suuntainen salasanapohjainen autentikointi, ei tarvetta sertifikaateille)
- Protected Extensible Authentication Protocol (PEAP) (Luo ensin turvallisen TLS-tunnelin, jonka kautta autentikointi suoritetaan, vaatii sertifikaatin palvelimelle)
- Tunneled Transport Layer Security (TTLS) (Samantapainen toteutus kuin PEAP, asiakaskone ei tarvitse sertifikaattia)
- Ciscon Flexible Authentication via Secure Tunneling (FAST) (Luo ensin turvallisen tunnelin, jota käytetään 2 suuntaiseen autentikointiin).

Huomioitavaa on, että verkkoon liittyvän asiakaslaitteen sekä verkkolaitteiden on tuettava samaa EAP-protokollaa, jotta valitun menetelmän käyttö olisi ylipäätään mahdollista. (Wi-Fi Alliance 2009 7; Airmagnet n.d 4-5.)

5 Ekokem PÄÄKONTTORIN LANGATON VERKKORATKAISU

Seuraavassa vaiheessa edellä läpikäydyn teorian pohjalta määritellään Ekokem Oy Ab pääkonttorin tiloihin soveltuva ja asetetut tavoitteet täytävä/ylittävä WLAN-verkkoratkaisu. Työni tukena hyödynnän Riihimäen ammattikorkeakoulusta jo valmistuneen Laakson Tonin Ekokemille 2010 tekemää opinnäytetyötä. Toni on tuolloin suorittanut pääkonttorille suunnitellun WLAN-verkon kartoituksen. Kartoituksen yhteydessä on suoritettu kuuluvuusmittauksia ja näin saatu muodostettua kuva siitä kuinka monta tukiasemaa verkon peittoalueen saavuttamiseen vaaditaan. Samalla on kirjattu ylös verkon määrittely koskien: peittoaluetta, käyttötarkoitusta, käyttäjämääriä, nopeusluokkaa ja tietoturvaa.

Määrittely vaiheen lopuksi tulen laatimaan dokumentin, joka sisältää mahdollisimman tarkan kuvauksen määritellystä WLAN-verkosta. Tähän dokumenttiin liite 1 perustuen tulen kontaktoimaan ja pyytämään WLAN-verkkoratkaisuja ja tarjouksia operaattoreilta ja laitetoimittajilta. Työn lopuksi tulen vertailemaan saamiani ratkaisuehdotuksia ja teen niistä yhteenvedot ja oman suositukseni.

5.1 WLAN-verkon määrittely

Ekokem Oy Ab pääkonttorille Riihimäkeen suunnitellun WLAN-verkon tarkoitus on laajentaa koko konttorin kattava langallinen tietoliikenneverkko palvelemaan joustavammin liikkuvia käyttäjiä. Nykyinen langallinen verkko on toteutukseltaan osin 100 Mbps ja osin 1000 Mbps. WLAN-verkolla haetaan joustavuutta kannettavilla tietokoneilla työskenteleville työntekijöille, sekä mahdollisuus tarjota vieraille yhteys julkiseen verkkoon.

Aikaisemmin suoritetussa kartoituksessa on päädytty 802.11g-standardin laitteiden riittävän tarjoamaan tarvittava tiedonsiirtonopeus. Koska laitteiden hinnat ovat viimeisen vuoden aikana tulleet merkittävästi alaspäin, niin toteutuksessa voi tulla kyseeseen myös 802.11n-standardin laitteet. Aikaisemman kartoituksen perusteella on myös päädytty 9 tukiaseman riittävän verkon peittoalueen kattamiseksi. Suunnitellun verkon hallinta tulisi yksittäisten tukiasemien sijaan toteuttaa keskitetysti, ettei verkonhallinta merkittävästi lisäisi IT teknisentuen työmäärää. Tietoturva näkökulmasta on salaus päätetty toteuttaa WPA2-menetelmillä, mutta autentikointi olisi mielestäni jaetun avaimen sijaan tuotantoverkossa syytä toteuttaa 802.1X-menetelmillä. (Toni 2010 14.)

Toni on työssään suorittanut konttorin sisätiloissa mittaukset 802.11g-standardin tukiasemilla Linksys WRT610N ja Ekohau HeatMapper ohjelmalla. Olen katsonut näiden tulosten toimivan hyvin työssäni verkon peittoaluetta ja tukiasemien määrää arvioitaessa. Verkon peittoalueelle asetetut määritykset ovat säilyneet samoina, kuten ne on viime vuonna määritetty. Verkon peittoalue ja tukiasemien sijainnit käyvät selville liitteestä 1. WLAN-verkon toteutusvaiheessa on vielä syytä suorittaa katselmus ja mittauksia, jotta voidaan varmistua halutunlaisen tuloksen saavutuksesta. (Toni 2010.)

5.2 Daimler Finlandin tarjous

Daimler tarjoaa toteutettavan WLAN-verkon laitteiksi Ruckus Wireless valmistajan tukiasemia 9 kpl ja kontrolleria. Tarjottu kontrolleri millä verkkoa hallitaan keskitetysti, on malliltaan Ruckus ZoneDirector 1112. Peruslisenssillä laite tukee 1-12 tukiaseman verkkoa. Laite on ohjelmistopohjaisesti päivitettävissä, jopa 50 tukiasemaan asti. Kontrollerissa on 2 kappaletta Gigabitin ethernet-porttia verkkoliikenteelle. Tukiasemiksi on tarjottu mallia Ruckus 7341. Tukiasema on 802.11n-standardiin perustuva, tarjoten 300 Mbps maksimi tiedonsiirtonopeuksia. Laite on varustettu yhdellä 2,4 GHz taajuusalueella toimivalla radiolla ja antenniratkaisu on älykäs itsesuuntaava. Tukiasemassa on yksi Gigabitin ethernet-portti ja virransyöttö onnistuu Power over Ethernet (PoE)-ratkaisulla tai erillisellä virtalähteellä. Tarjoukseen on liitetty tukiasemille PoE Injector virtalähteet, joilla virransyöttö voidaan toteuttaa laitteeseen liitettävää ethernet-kaapelia pitkin. Kontrollerilla ja tukiasemilla on elinikäinen takuu. (ZoneFlex 2011; ZoneDirector 2010.)

Optioina on tarjolla support-palveluita, jotka sisältävät teknisentuen 24/7/365, ohjelmistopäivitykset, laitteiden nopean takuuvaihdon. Daimler suosittelee ottamaan kontrollerille vähintään kolmen vuoden supportin. Tukiasemillekin on saatavilla support-palveluita. Tarvittaessa Daimler tarjoaa myös asennus- ja laitteiden konfigurointipalvelua.

Ruckus Wireless WLAN-ratkaisun eduista mainittakoon älykäs BeamFlex itsesuuntaava antennitekniikka, joka mahdollistaa pidemmän kantaman ja toimintavarman ympäristön. BeamFlex-antenni kohdistaa automaattisesti signaalin päätelaitteen suuntaan ja mukautuu päätelaitteen liikkeeseen. SmartMesh toiminto tukiaseman langatonta runkoyhteyttä varten tiloihin, joissa ei ole lähiverkkokaapelointia. Kontrolleri säätää ja optimoi langattoman Mesh-verkon reitityksen automaattisesti. Tietoturva on toteutettavissa helposti, mutta turvallisesti esimerkiksi Ruckuksen patentoimalla dynaamisella PSK-menetelmällä. Menetelmässä jokainen verkkoon liittyvä käyttäjä tunnistetaan salatun web-sivun kautta Active Directorya vastaan ja sen jälkeen automaattinen scripti tekee käyttäjän koneelle tarvittavat asetukset langattomalle yhteydelle. Jokainen käyttäjä saa oman uniikin salausavaimen. Verkon käyttöönotto ja konfigurointi on tehty erittäin helpoksi ja nopeaksi Wizard-asetusohjelmalla. (Daimler n.d; Ruckus Wireless 2009.)

5.3 Nylund Group tarjous

Nylund tarjoaa WLAN-verkon toteutukseen Juniper merkkisiä laitteita. Verkon keskitettyyn hallintaan Juniperin WLC8 mallista kontrolleria, jolla voidaan hallita 1-12 tukiaseman verkkoa. WLC8 kontrolleri ei ole laajennettavissa, mutta sitä voidaan hyödyntää verkkoa laajennettaessa klusterin osana. Klusteroinnilla saadaan jopa 64 laitetta näkymään yhtenä virtuaalikontrollerina. Kontrollerissa on 8 kappaletta 100 Mbps ethernet-porttia verkkoliikenteelle, joista 6 porttia tukee PoE virransyöttöä. Vikasietoisuuden lisäämiseksi kontrolleria on saatavilla kahdella virtalähteellä. Tukiasemiksi on tarjottu 9 kpl Juniper WLA522, joka tukee 802.11n-standardia ja on varustettu kahdella radiolla. Dual radion ansiosta tukiasema toimii molemmilla eli 2,4 GHz ja 5 GHz taajuuksilla. Tiedonsiirtonopeus maksimissaan 300 Mbps per radio. Tukiaseman antenniratkaisu on 2x2 MIMO ja antennit ovat ympärisäteileviä. Tukiasemassa on yksi Gigabitin ethernet-portti ja virransyöttö laitteelle tapahtuu PoE-menetelmällä. Virransyöttö toteutetaan siis kontrollerin portista tai erillisellä PoE Injector virtalähteellä. Kontrollerilla on 90 päivän takuu ohjelmistolle ja vuoden takuu raudalle. Takuu on huoltosopimuksilla laajennettavissa. Tukiasemalla on rajoitettu elinikäinen takuu eli käytännössä 5 vuotta tuotteen valmistuksen päättymisestä. (WLC datasheet n.d, WLA datasheet n.d.)

Optioina on tarjolla support-palveluita tarjotuille laitteille ja ohjelmistoille. Supportit sisältävät teknisentuen, päivitykset, webpohjaisen tukitietokannan 24/7/365. Verkon toteutukseen tarvittavien laitteiden lisäksi tarjotaan erillistä RingMaster-ohjelmistoa helpottamaan verkon konfigurointia, ylläpitoa, suunnittelua ja raportointia. Lisäksi vierailijatunnusten luontiin on tarjolla erillinen SmartPass-ohjelmisto, jonka avulla esimerkiksi vastaanottovirkailija voi luoda vierailijatunnuksia. SmartPass toimii käytännössä RADIUS-palvelimena.

Tarjotun ratkaisun eduista mainittakoon tuotteiden modulaarisuus eli mahdollisesti hankittavat lisäpalvelut ja laitteet on helposti liitettävissä jo olemassa olevaan WLAN-verkkoon. Laitteilla on myös mahdollista toteuttaa langaton Mesh-verkko jolloin runkoyhteys tukiasemalle voidaan toteuttaa langattomasti. Kontrolleri osaa itse säätää reitityksen Mesh-verkossa. Tukiasemia on myös mahdollista hyödyntää siltaavina eli näin saadaan verkot liitettyä toisiinsa langattomasti. Kontrolleri on konfiguroitavissa oman komentopohjaisen käyttöliittymänsä kautta, selaimella tai optiona saatavalla RingMaster-hallintaohjelmistolla. WLAN-verkkoon liittyvien käyttäjien autentikointi voidaan toteuttaa esimerkiksi Web-Portal sivustolla. Tällöin verkkoon liittyvät käyttäjät ohjautuvat kirjautumissivulle, jossa kysellään käyttäjätunnus ja salasana. Tunnuksia verrataan kontrollerin paikalliseen tietokantaan tai RADIUS-palvelimen tietokantaan.

Verkkoratkaisun tukiasemat on varustettu kahdella radiolla ja näin laite voi esimerkiksi palvella vanhemman standardin laitteita 2,4 GHz taajuudella ja ohjata uudemmat n-standardin laitteet 5 GHz taajuudelle. Tukiasemat eivät sisällä muuta kuin käynnistysohjelmiston eli konfigurointitiedot kuten salausavaimet tulevat aina kontrollerilta. Näin ollen tukiasema on varastettuna täysin hyödytön ja sen mukana ei menetetä mitään tärkeitä tietoja. (WLA datasheet n.d, Juniper Networks n.d.)

5.4 Elisan tarjous

Elisan tekemässä tarjouksessa WLAN-verkon toteutukseen tarjotaan Ciscon kontrolleria ja tukiasemia. Kontrolleri on malliltaan Cisco 5508, joka tukee 12 tukiaseman verkkoa ja on laajennettavissa lisensseillä aina 500 tukiasemaan asti. Laitteessa on 8 kappaletta Gigabitin ethernet-porttia verkkoliikenteelle. Vikasietoisuutta lisäämään laitteeseen on mahdollista asentaa lisävirtalähde. Verkkoratkaisun tukiasemiksi Elisa tarjoaa 9 kpl Ciscon 1041 Lightweight Access Point (LAP) eli tukiaseman kevyttä versiota, joka toimii vain kontrollerin hallitsemassa verkossa. Tukiaseman verkkoliitäntä on Gigabitin ethernet-portti ja virransyöttö laitteelle toteutetaan PoE-menetelmällä tai erillisellä virtalähteellä. Tarjoukseen on liitetty PoE Injector virtalähteet virransyöttöä varten. Tukiasema on varustettu yhdellä 2,4 GHz radiolla ja tiedonsiirtonopeus on maksimissaan 300 Mbps. Laitteen antenniratkaisu on 2x2 MIMO ympärisäteilevillä antenneilla. Kontrollerilla on valmistajan 90 päivän takuu ja tukiasemilla rajoitettu elinikäinen takuu. (Cisco WLC n.d; Cisco AP n.d.)

Elisa tarjoaa edellä esitellylle WLAN-verkon toteutukselle kahta hallintamalliratkaisua riippuen siitä suoritetaanko verkonhallinta itse vai ostetaan se palveluna Elisalta. Jos palvelu ostettaisiin kokonaan Elisalta, se sisältäisi Tukiasema- ja Vierailijaverkkopalvelun. Palveluun kuuluu Elisan 10M internet-yhteyden asennus ja avaus, tukiasemien ja kontrollerin asennus, sekä tukiasemakohtainen WLAN-palvelu. Jos verkon konfigurointi ja hallinnointi suoritetaan itse, niin Elisalta saisi kattavat huolto- ja varalaittepalvelut.

Ratkaisussa tarjottu Ciscon kontrolleri on erittäin laadukas ja hyvin skaalautuva suurienkin WLAN-verkkojen hallintaan. Laite itsessään sisältää monipuoliset ja nopeat Gigabitin verkkoliitännät ja laajennuspaikan lisäliitännöille. Asetukset tehdään joko komentopohjaisen käyttöliittymän kautta tai selkeän selainpohjaisen portaalin kautta. Moninaiset asetusparametrit mahdollistavat WLAN-verkon monipuolisen räätälöinnin. WLAN-verkon käyttäjien tietoturva voidaan toteuttaa esimerkiksi Ciscon omalla EAP-FAST-menetelmällä, jolloin käyttäjätietokantana voidaan hyödyntää suoraan Active Directorya LDAP-protokollan avulla. Tukiasemien runkoyhteydet voidaan myös toteuttaa langattomasti Mesh-verkkona, jos tukiasemalle ei ole langallista verkkoyhteyttä. Verkkoratkaisun tukiasemat toimivat ainoastaan kontrollerin hallitsemassa verkossa eli tukiasema saa kaikki asetuksensa kontrollerilta ja on näin ollen täysin hyödytön joutuessaan väärin käsiin. (Cisco WLC n.d; Cisco AP n.d.)

5.5 AinaCom tarjous

AinaComin tarjous perustuu myös verkkolaittevalmistaja Ciscon laitteisiin. Kontrolleriksi on tarjottu samaa 5508 mallia, joka on esitelty jo Elisan tarjouksen yhteydessä. Tukiasemien osalta AinaCom tarjoaa 9 kpl Ciscon 1141 LAP eli tukiaseman kevyttä versiota, joka toimii vain kontrollerin hallitsemassa verkossa. Ciscon 1140-sarjan tukiasema eroaa Elisan tarjoamasta Ciscon 1040-sarjasta käytännössä vain antenniratkaisullaan. 1140 antenniratkaisu on MIMO 2x3 eli kaksi lähettävää ja kolme vastaanotto antennia. Tällä ratkaisulla saadaan hiukan kasvatettua kantomatkaa ja vikasietoisuutta, jos ympäristössä on paljon häiritsevää radioliikennettä. Tukiaseman verkkoliitäntä on Gigabitin ethernet-portti ja virransyöttö laitteelle toteutetaan PoE-menetelmällä tai erillisellä virtalähteellä. Kontrollerilla on valmistajan 90 päivän takuu ja tukiasemilla rajoitettu elinikäinen takuu. (Cisco WLC n.d; Used Cisco n.d.)

Optioina AinaCom tarjoaa verkon ylläpitopalvelua, joka sisältäisi verkon alkukonfiguraatiot ja jatkossa suoritettavat muutokset toimenpiteet. Palvelu sisältäisi myös kontrollerin huoltopalvelun 5 päivänä viikossa 8 tuntia päivässä 4 tunnin vasteajalla.

Ominaisuuksiltaan AinaComin tarjouksen sisältämät laitteet ovat käytännössä katsoen samanlaiset kuin Elisan tarjouksessa. Tarjouksen etuina mainittakoon laadukkaat Ciscon laitteet, joilla verkon ylläpito onnistuisi Ekokemin oman IT-henkilökunnan toimin, aiheuttamatta suurta työkuormaa. Optiona saatavalla ylläpitopalvelulla verkon toiminnallisuus ja ylläpito saataisiin myös toteutettua varsin edullisesti. Ylläpitosopimuksen sisältämä kontrollerin huoltopalvelu myös helpottaisi mahdollisten laitevikojen sattuessa.

5.6 LAN&WAN Nordic tarjous

LAN&WAN tarjouksen laitteisto koostuu Motorolan tukiasemista 9 kpl AP650 ja kontrollerista RFS6000. Kontrollerilla voidaan hallita 16 AP650 mallisen tukiaseman verkkoa, joka on myöhemmin lisensseillä laajennettavissa 48 tukiasemaan asti. Kontrollereita on myös mahdollisuus yhdistellä isommaksi klusteriksi, jolloin 12 kontrollerin klusteri tukee jopa 576 tukiasemaa. Laitteessa on 8 kappaletta Gigabitin ethernet-portteja verkkoliikenteelle PoE virransyötöllä ja yksi Gigabitin kuituliitäntä runkoyhteydelle. Mainittakoon verkkoliitännöistä vielä ExpressCard-liitäntä, joka mahdollistaa 3G-modeemin käytön vararunkoyhteytenä. Tukiasemiksi on tarjottu AP 650 mallin sisäisillä antennilla ja kahdella radiolla varustettua versiota. Tukiasema on 802.11n-standardiin perustuva tarjoten 300 Mbps maksimi tiedonsiirtonopeuksia 2,4 GHz sekä 5 GHz taajuuksilla toimivilla radioilla. Antenniratkaisu on MIMO 2x3 eli kaksi lähettävää ja kolme vastaanotto antennia. Tukiasemassa on 1 Gigabitin ethernet-liitäntä ja virran syöttö onnistuu PoE-menetelmällä verkkokaapelia pitkin. (RFS 6000 2009; AP 650 2010.)

LAN&WAN tarjouksessa on esitelty kahdenlaista ratkaisuvaihtoehtoa, joista toinen on avaimet käteen tyyppinen palvelu ja toinen ratkaisu sisältäisi WLAN-verkon laitteet sekä huoltopalvelun. LAN&WAN tarjoamana kokonaisvaltaisena WLAN-Palveluna WLAN-verkon kaikki laitteet, tukipalvelut, hallinnointi ja verkon kehittäminen sisältyisivät kiinteään kuukausihintaan. Toisena vaihtoehtona on ostaa tukiasemat ja kontrolleri, sekä hoitaa verkon konfiguroinnit ja hallinnointi itse. Tähän vaihtoehtoon LAN&WAN tarjoaisi kiinteällä kuukausihinnalla huoltopalvelua, joka sisältäisi huollon ja puhelintuen koskien laitteistoa ja sen käyttöä arkisin klo 8-16.

Tarjotun laitteiston eduista on huomioitava ensinnäkin Motorolan RFS6000 kontrollerin hinta vs. ominaisuudet. Kontrolleri on kilpailijoihin verrattuna edullisen hintansa lisäksi varustettu monipuolisilla ja nopeilla verkkoliitännöillä, sekä kontrollerin web-käyttöliittymä eli Wi-NG tekee alkukonfiguraatioiden asetuksen selkeäksi ja verkon jokapäiväisestä hallinnoinnista helppoa. Klusterointi taas mahdollistaisi WLAN-verkon laajentamisen ja tekisi uusien laitteiden lisäämisen helpoksi. Tietoturva on toteutettavissa esimerkiksi kontrollerin sisäisen RADIUS-palvelimen avulla, joka tukee yleisimpiä 802.1X EAP-autentikointimenetelmiä. Tällöin käyttäjätietokantana voitaisiin hyödyntää vaikka jo olemassa olevaa Active Directorya LDAP-protokollan avulla. Vikasietoisuuden lisäämiseksi on useita toimintoja kuten 3G-modeemin käyttö vararunkoyhteytenä, sekä WLAN-verkon self healing menetelmä jolloin naapuri tukiasema pyrkii automaattisesti paikkaamaan vikaantunutta tukiasemaa. Tarjotut tukiasemat AP650 ovat plug&play tyyppisiä laitteita eli ne vain kytetään verkkoon, jolloin kontrolleri löytää ne ja lataa niihin tarvittavat ohjelmistot ja asetukset. Tällä laiteratkaisulla verkon hallinnointi onnistuisi varmasti varsin pienellä työmäärällä myös Ekokemin omalta IT-henkilökunnalta. Laiteratkaisun lisäksi olisi järkevää ottaa vielä LAN&WAN tarjoama pronssitason huoltopalvelu. (Wing system reference guide 2009.)

5.7 Suositukset

Tutustuttuani tarkoin edellä esiteltyihin tarjouksiin ja laiteratkaisuihin olen omaan asiantuntemukseeni ja asetettuihin WLAN-verkon määrittelyihin liite 1 tukeutuen muodostanut näkemyksen juuri Ekokemille sopivasta ratkaisusta. Tarjouksia pyydettiin yhteensä viisi kappaletta, joista jokainen sisältää laadukkaan laiteratkaisun halutunlaisen WLAN-verkon toteuttamiseen. Tarjottujen laitekokonaisuuksien arvioimiseksi tutustuin jokaisen laitteen asennus ja konfigurointi käsikirjoihin. Arviointini laitteiden osalta perustuu helppokäyttöisyyteen ja monipuolisiin fyysisiin ja ohjelmallisiin ominaisuuksiin. Huomioitavaa on, että en ole laitteita päässyt käytännössä kokeilemaan vaan arvioni perustuvat teknisiin tietoihin mitä laitevalmistajien dokumentoinneista selviää. Tarjotut laiteratkaisut ovat joka tapauksessa tunnettujen ja luotettavien yritysten ammattilaisten tekemiin suosituksiin perustuvia kokonaisuuksia ja siten pelkoa huonolaatuisista laitteista ei ole.

LAN&WAN Nordicin tarjoama Motorolan laiteratkaisu on tutkimusteni perusteella varteenotettavin vaihtoehto juuri Ekokemin pääkonttorin nykyisen verkkoympäristön laajennukseksi ja käyttötarkoitus huomioiden. Motorolan kontrolleri vaikuttaa helppokäyttöiseltä selkeän web-käyttöliittymänsä ansiosta ja laite itsessään sisältää hintaluokkaansa nähden monia sellaisia toimintoja mitä muista samanhintaisista laitteista ei löydy tai ne ovat saatavina erillisinä lisäpalveluina. Motorolan kontrolleria voisi ominaisuuksiltaan verrata noin 2000 € kalliimpaan Ciscon 5508 laitteeseen, jota Elisa ja AinaCom tarjoavat. Kontrollerin ulkoisista ominaisuuksista on huomioitava monipuoliset ja nopeat verkkoliitännät, jotka mahdollistavat nopean tiedonsiirron ja kapasiteettia on jo valmiiksi tulevaisuudenkin tarpeita varten. Laitteessa on myös monia valmiiksi sisäänrakennettuja toimintoja, joista tärkeimpänä mainittakoon sisäinen RADIUS-palvelin. Tämä mahdollistaisi käyttäjien vahvan autentikoinnin, käyttöoikeuksien hallinnan ja liikenteen seurannan ilman erillisen palvelinraudan ja palveluiden virittelyä.

WLAN-verkon tukiasemia valittaessa on mahdollisuus ostaa joko yhdellä tai kahdella radiolla varustettuja tukiasemia. Hintaeroa tukiasemille jää vain noin 90 € eli suorituskyky ja hintaero huomioiden järkevää olisi valita suoraan dual radio tukiasemat. Näin esimerkiksi ruuhkatilanteissa vanhemmat laitteet käyttävät 2,4 GHz taajuutta ja uudemmat 5 GHz taajuutta. Tietysti on myös mahdollista tehdä kompromissi ja ostaa dual radio tukiasemat paikkoihin joissa käyttäjämäärät ovat suurempia kuten pohjoissiipi, eteläsiipi ja neuvottelutilat. Loput voisivat sitten olla yhdellä radiolla varustettuja tukiasemia.

Tälle laitteistoratkaisulle LAN&WAN tarjoaisi pronssitason huoltopalvelua kohtuullisella kuukausiveloituksella. Huoltopalvelu olisi ainakin aluksi syytä ottaa jo pelkän puhelintuen takia eli tällöin laitteistoa ja sen käyttöä koskeviin ongelmiin olisi saatavilla asiantuntevaa apua arkisin klo 8.00 – 16.00. Lisäksi huoltopalvelu sisältää laitteiston huollot, varaosat ja tarvittaessa vaihtolaitteen. Huoltopalvelun tarpeellisuutta voisi jatkossa miettiä tarkemmin, kunhan ensin näkee laitteiston toiminnassa ja opettelee hallinnoimaan WLAN-verkkoa. Huoltopalvelun tarvetta voidaan myös arvioida WLAN-verkon kriittisyys huomioon ottaen siten, että pidemmällä aikavälillä 6kk-12kk seurataan kuinka paljon katkoksia tapahtuu ja tulosten perusteella määritellään missä kipuraja kulkee. Ekokemillä on kuitenkin olemassa jo toimiva ja laaja langallinen verkko, jolloin työnteke ei täysin esty vaikka langaton verkko olisikin hetkellisesti kokonaan tai osittain poissa käytöstä.

6 YHTEENVETO

Yhtenä tämän opinnäytetyön tavoitteista oli tutustua uusiin langattomiin WLAN- sekä 4G-standardeihin. Teorian läpikäynti oli hyvin palkitsevaa, mutta osittain työlästä, sillä suurin osa tutkimusmateriaaleistani oli englanninkielistä. Alun teoriaosa syvensi tietämystäni erilaisista langattomista tekniikoista ja antoi ammatillisessa mielessä hyvän katsauksen nykytilanteesta ja tulevaisuuden näkymistä. Mielestäni onnistuin pitämään teoriaosuuden johdonmukaisena ja maallikonkin helposti ymmärrettävässä muodossa.

Teoriaosuuden jälkeen oli huomattavasti helpompi lähteä toteuttamaan varsinaista fyysistä osuutta eli verkon määrittelyä, tarjouspyyntöjen laatimista ja tarjousten vertailua. Verkon määrittelyn pohjana pystyin hyvin hyödyntämään 2010 Ekokemillä työskennelleen Toni Laakson Wlanin kartoitus opinnäytetyötä. Näin minun ei tarvinnut lähteä liikkeelle aivan tyhjältä pöydältä ja aikaa säästy. WLAN-verkon määrittelydokumentin liite 1 koostaminen onnistui Tonin esityön ja oman työni teoriaosuuden pohjalta melko mutkattomasti. Muutamia asioita piti hiukan päivittää, sillä tekniikan osalta etenkin n-standardin laitteiden hinnat ovat viimeisen vuoden aikana tulleet huomattavasti alaspäin. Lisäksi otin edeltäjäni tiukemman näkökulman koskien tietoturvaa ja verkon hallintaa, sillä lähtökohtana oli kuitenkin yrityksen tuotantoverkkoon liitettävä osa.

Seuraavassa vaiheessa oli sitten tutustuttava tarkemmin saapuneisiin tarjouksiin ja tarjousten sisältämiin laitteistoratkaisuihin. Tämä oli varmasti työni työläin vaihe, koska laitteiden dokumentit ovat lähes poikkeuksetta englanninkielisiä ja sivumääriltään massiivisia teoksia. Tarkoitukseni oli ottaa jokaisesta laiteratkaisusta esille keskeisimmät suorituskykyä ja ominaisuuksia kuvaavat tiedot joiden perusteella päätöksenteko ratkaisua valittaessa olisi helpompaa. Tämä oli mielenkiintoinen vaihe sillä viidestä tarjouksesta neljä koostui eri laitevalmistajan ratkaisusta. Laitteiden konfiguraatio- ja asennusdokumentteihin tutustuminen antoi kyllä selkeän kuvan kustakin laitteistoratkaisusta ja oli mielenkiintoista havaita, että kuinka erilaisilla samaan standardiin perustuvat toiminnot voidaan tehdä ja toteuttaa.

Viimeisessä vaiheessa esittelin ja perustelin omaan asiantuntemukseeni ja teoriatietoon perustuen varteenotettavimman tarjouksen Ekokemin WLAN-ratkaisuksi. Tämä oli kohtalaisen helppo osuus sillä tarjouksiin tutustuttuani yksi nousi selkeästi yli muiden niin hintansa kuin ominaisuuksiensa puolesta.

Kokonaisuutena ajatellen opinnäytetyö onnistui hyvin alussa tekemääni työsuunnitelmaa mukaillen. Työn suorittamiseen varaamani aika tuntui aluksi hiukan liioitellulta, mutta kesän muiden työkiireiden keskellä aika kuluikin sitten yllättävän nopeasti. Itse koen onnistuneeni täyttämään työn aloitusvaiheessa toimeksiantajan kanssa sovitut vaatimukset. Mielellään olisin halunnut myös päästä näkemään millaiseen ratkaisuun Ekokemillä tullaan loppujenlopuksi päättämään ja mikä minun esityöni todellinen painoarvo on.

LÄHTEET

- IEEE 802.11g 2003. Broadcom. Viitattu 23.6.2011.
<http://www.cse.iitb.ac.in/synerg/lib/exe/fetch.php?id=public%3Astudents%3Aadvait%3Ahome&cache=cache&media=public:students:advait:802.11g-wp104-r.pdf>
- Cisco Systems 2005. Capacity, coverage and deployment considerations for IEEE 802.11g Viitattu 23.6.2011.
http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_white_paper09186a00801d61a3.shtml
- Industrial Scientific and Medical (ISM) Bands 1993. Wireless Communication. Viitattu 28.9.2011.
<http://wireless.per.nl/reference/chaptr01/dtmmsyst/ism.htm>
- WLAN n.d. Phoenix Contact Oy. Viitattu 25.6.2011.
http://www.phoenixcontact.fi/technologies/18699_18716.htm
- Channels for 802.11g n.d. Air-stream. Viitattu 25.6.2011.
http://www.air-stream.org.au/channel_802_11g
- 802.11n primer 2008. Airmagnet. Viitattu 26.6.2011.
<http://airmagnet.flukenetworks.com/products/whitepaper/download.php?dwn=WP-802.11nPrimer.pdf>
- Paul DeBeasi 2008. 802.11n: Enterprise Deployment Considerations. Viitattu 27.6.2011.
http://www.wi-fi.org/knowledge_center_overview.php?docid=4568
- Connect 802 n.d. Understanding 20 MHz Versus 40 MHz 802.11n Channel Configuration. Viitattu 27.6.2011.
http://www.connect802.com/80211n_channels.htm
- Alcatel n.d. WiMAX making ubiquitous high-speed data services a reality. Viitattu 2.7.2011.
<http://www.scribd.com/doc/14024413/Alcatel-Wimax-Whitepaper>
- Mobile WiMAX n.d. Sprint. Viitattu 2.7.2011.
<http://www.wimax.com/whitepapers/sprint-mobile-wimax.pdf>
- Tejas Bhandare 2008. LTE and WiMAX Comparison. Viitattu 2.7.2011.
<http://www.pixaware.com/LTE%20and%20WiMAX%20Comparison-TejasBhandare.pdf>
- Radio-electronics n.d. LTE OFDM, OFDMA and SC-FDMA. Viitattu 4.7.2011.
<http://www.radio-electronics.com/info/cellulartelecomms/lte-long-term-evolution/lte-ofdm-ofdma-scfdma.php>

WiMAX forum 2009. WiMAX, HSPA+, and LTE: A Comparative Analysis. Viitattu 4.7.2011.
http://wimaxforum.org/sites/wimaxforum.org/files/document_library/wimax_hspa+and_lte_111809_final.pdf

Tietokone 2010. Sonera: 4g-verkko Kehä I:n kattavaksi 2011. Viitattu 4.7.2011.
http://www.tietokone.fi/uutiset/sonera_4g_verkko_keha_i_n_kattavaksi_2011

Proessori 2009. LTE-päätelaitteita viiteen eri luokkaan. Viitattu 4.7.2011.
<http://www.proessori.fi/uutiset/uutinen2.asp?id=53546>

Networkworld 2010. `WiMAX 2` coming in 2011?. Viitattu 6.7.2011.
<http://www.networkworld.com/news/2010/012810-wimax-2.html?hpg1=bn>

TATA n.d. LTE-Advanced: Future of Mobile Broadband. Viitattu 6.7.2011.
http://www.tcs.com/SiteCollectionDocuments/White%20Papers/EIS_Whitepaper_LTE_Advanced_Future_of_Mobile_broadband_09_2009.pdf

Airmagnet n.d. Best Practices for Securing Your Wireless LAN. Viitattu 16.7.2011.
http://airmagnet.flukenetworks.com/products/whitepaper/download.php?dwn=WLAN_Security_Best_Practices.pdf

Wi-Fi Alliance 2009. The State of Wi-Fi Security. Viitattu 16.7.2011.
http://www.wi-fi.org/register.php?file=wp_State_of_Wi-Fi_Security_090911.pdf

Proessori 2011. Wimax hengittää vielä. Viitattu 1.8.2011.
<http://www.proessori.fi/uutiset/uutinen2.asp?id=57891>

IEEE Standards Association 2011. IEEE Approves IEEE 802.16m. Viitattu 1.8.2011.
<http://standards.ieee.org/news/2011/80216m.html>

Toni ,L 2010. Wlanin kartoitus. Hämeen ammattikorkeakoulu. Tietoliikennetekniikan koulutusohjelma. Opinnäytetyö. Viitattu 3.8.2011

Cisco WLC 2009. Local EAP Authentication on the Wireless LAN Controller with EAP-FAST and LDAP Server Configuration Example. Viitattu 5.8.2011.
http://www.cisco.com/en/US/products/ps6366/products_configuration_example09186a008093f1b9.shtml

Daimler n.d. Ruckus Wireless. Viitattu 5.8.2011.
<http://www.daimler.fi/tuotteet/langattomat-verkot/wlan-verkot/ruckus-wireless>

Ruckus Wireless 2009. Securing Wireless LANs with LDAP.
Viitattu 5.8.2011.
http://pdf.ruckuscdn.com/appnotes/appnote_securing_wlan_ldap.pdf

ZoneFlex 2011. Ruckus Wireless. Viitattu 5.8.2011.
<http://support.ruckuswireless.com/documents/176-zoneflex-9-1-1-release-notes/download>

ZoneDirector 2010. Ruckus Wireless. Viitattu 5.8.2011.
<http://support.ruckuswireless.com/documents/164-zonedirector-release-9-1-user-guide/download>

WLC datasheet n.d. WLC series wireless lan controllers.
Viitattu 13.8.2011.
<http://www.juniper.net/us/en/local/pdf/datasheets/1000360-en.pdf>

WLA datasheet n.d. WLA series wireless lan access points.
Viitattu 13.8.2011
<http://www.juniper.net/us/en/local/pdf/datasheets/1000359-en.pdf>

Juniper Networks n.d. Mobility System Software. Viitattu 13.8.2011.
http://www.juniper.net/techpubs/en_US/release-independent/wireless/information-products/topic-collections/wireless-lan/software/mss-75-config.pdf

Cisco WLC n.d. Cisco 5500 Series Wireless Controllers.
Viitattu 15.8.2011.
http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps10315/data_sheet_c78-521631.html

Cisco AP n.d. Cisco Aironet 1040 Series Access Points.
Viitattu 15.8.2011.
http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps11203/data_sheet_c78-609338.html

Used Cisco n.d. The Insider's Guide to Cisco's New Releases.
Viitattu 18.8.2011.
<http://www.usedcisco.in/GuideToCisco/>

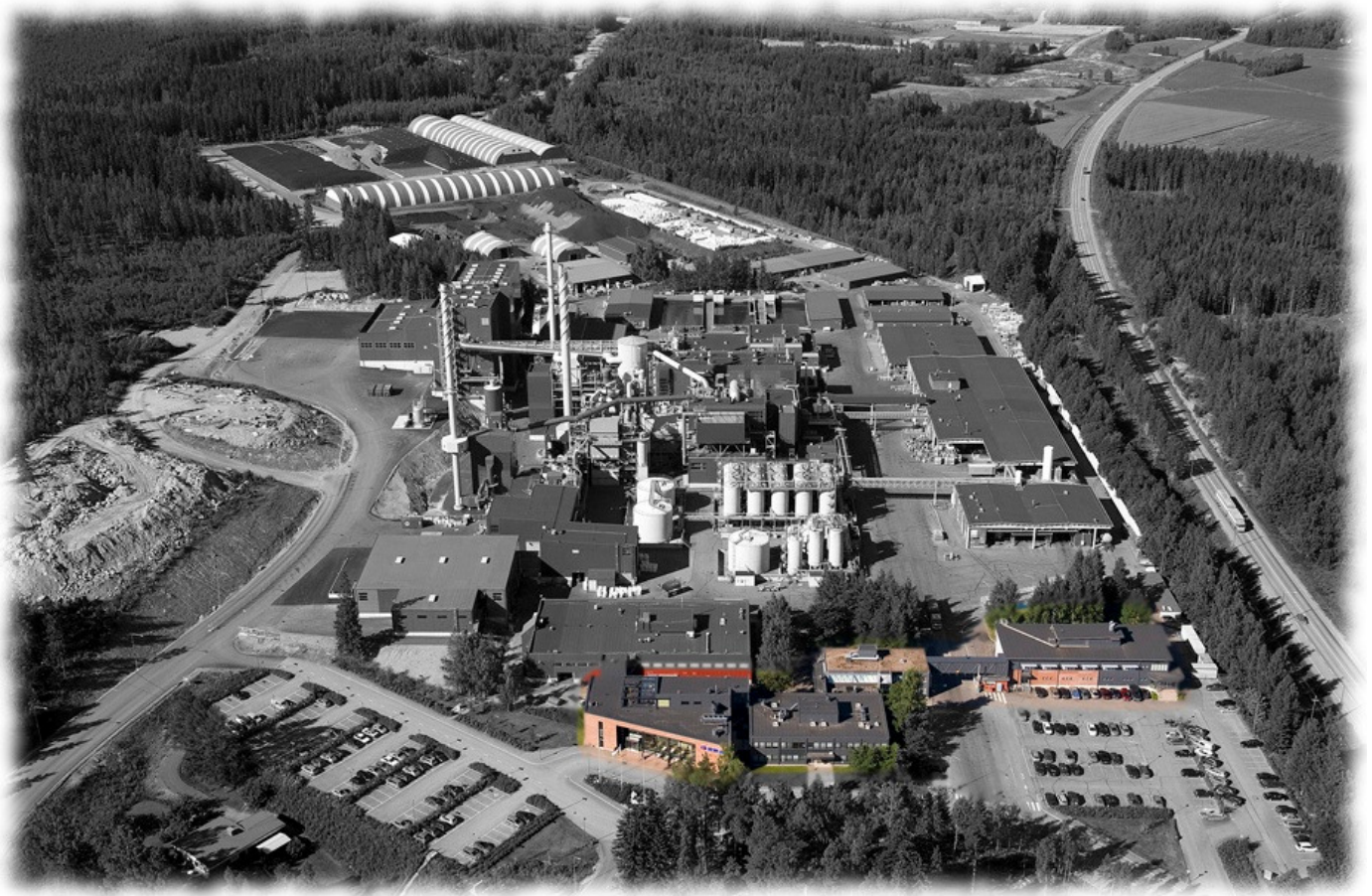
RFS 6000 2009. Wireless Services Controller. Viitattu 12.9.2011.
http://www.motorola.com/web/Business/Products/Wireless%20LAN%20Devices/Wireless%20Switches/RFS%206000/_Documents/RFS6000-SS-0309.pdf

AP 650 2010. 802.11n WLAN Access Point. Viitattu 12.9.2011.
http://www.motorola.com/web/Business/_Documents/Specifications/Static%20Flies/AP-650_Spec-Sheet_1010_chv3.pdf

Wing system reference guide 2009. Motorola RFS series LAN switches. Viitattu 14.9.2011.
<http://support.symbol.com/support/search.do?cmd=displayKC&docType=kc&externalId=12469001apdf&sliceId=&dialogID=247092884&stateId=1%200%20247086889>

WLAN-VERKON KUVAUS

Ekokem Oy Ab pääkonttorin WLAN



Kuulojankatu 1
11120 Riihimäki

Verkon käyttötarkoitus:

- Suunnitellun WLAN-verkon on tarkoitus toimia koko konttorin kattavan langallisen verkon laajennuksena, josta osa on 1Gbps ja osa 100Mbps verkkoa.
- WLAN-verkolla on tarkoitus saavuttaa joustavampi työympäristö kannettavilla tietokoneilla työskenteleville työntekijöille, jotka voisivat tarvittaessa ottaa koneensa työpisteeltään mukaan konttorin sisätiloissa liikkueessaan menettämättä verkkoyhteyksiä.
- Langattomalla verkolla on myös tarkoitus kattaa konttorin tiloissa sijaitsevat neuvottelutilat.
- Neuvottelutiloissa tulisi olla myös tuotantoverkosta eriytetty ”vierailijaverkko”, josta olisi yhteys vain julkiseen verkkoon.

Verkon määrittely:

- Konekanta ja aiheutuva verkkoliikenne huomioon ottaen 802.11g-standardin on katsottu täyttävän asetetut vaatimukset.
- Verkon käyttäjämäärät tulevat olemaan kohtalaisen pieniä ja arviolta enintään 10 tietokonetta per tukiasema.
- Kuuluvuusmittauksia on suoritettu aikaisemman kartoituksen yhteydessä 802.11g-standardin tukiasemilla (Linksys WRT610N) ja Ekohau HeatMapper ohjelmalla.
- Mittausten perusteella on päädytty 9 tukiaseman riittävän suunnitellun verkon toteuttamiseen.
- Salaus ja käyttäjien autentikointi on aikaisemmin päätetty toteuttaa WPA2-menetelmillä. Todennäköisesti kyseeseen tulisi kuitenkin jokin 802.1X-autentikointi WPA2-PSK:n sijaan.
- Verkon täytyisi olla keskitetysti hallittavissa, jotta se ei merkittävästi lisäisi IT teknisentuen työkuormaa.

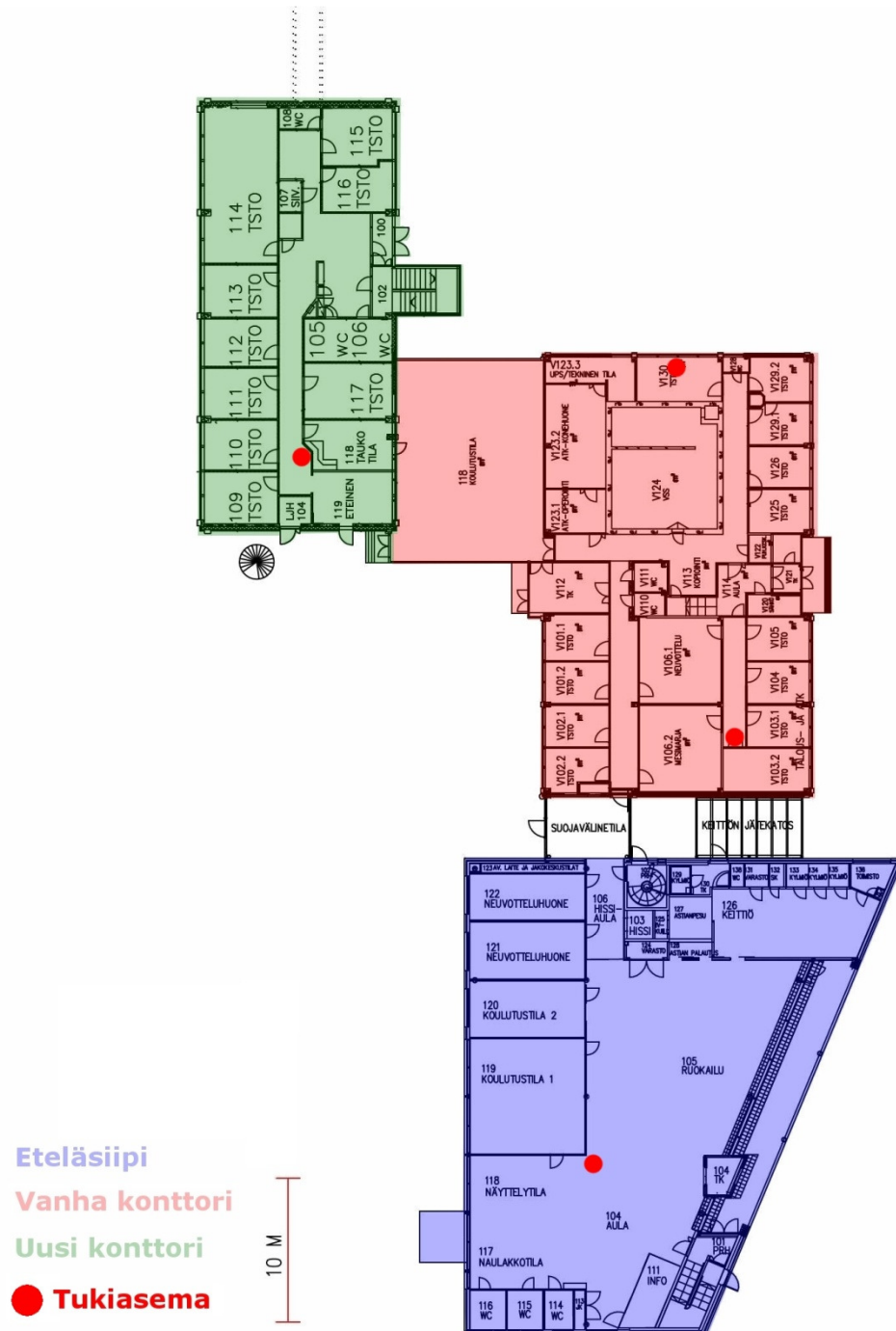
Verkon peittoalue:

- Konttorirakennus minne langatonta verkkoa ollaan suunnittelemassa, on pääosin kaksikerroksinen poikkeuksena kolmannen kerroksen edustustilat.
- Mittausten yhteydessä on huomioitu signaalia vaimentavat rakenteet kuten väestösuojat, rappukäytävät ja hissikuilu.
- Arkistotilat, eteläsiiven kellarikerros ja pohjoissiiven 1. kerroksen pukuhuoneet on myös jätetty pois verkon kuuluvuusalueesta.

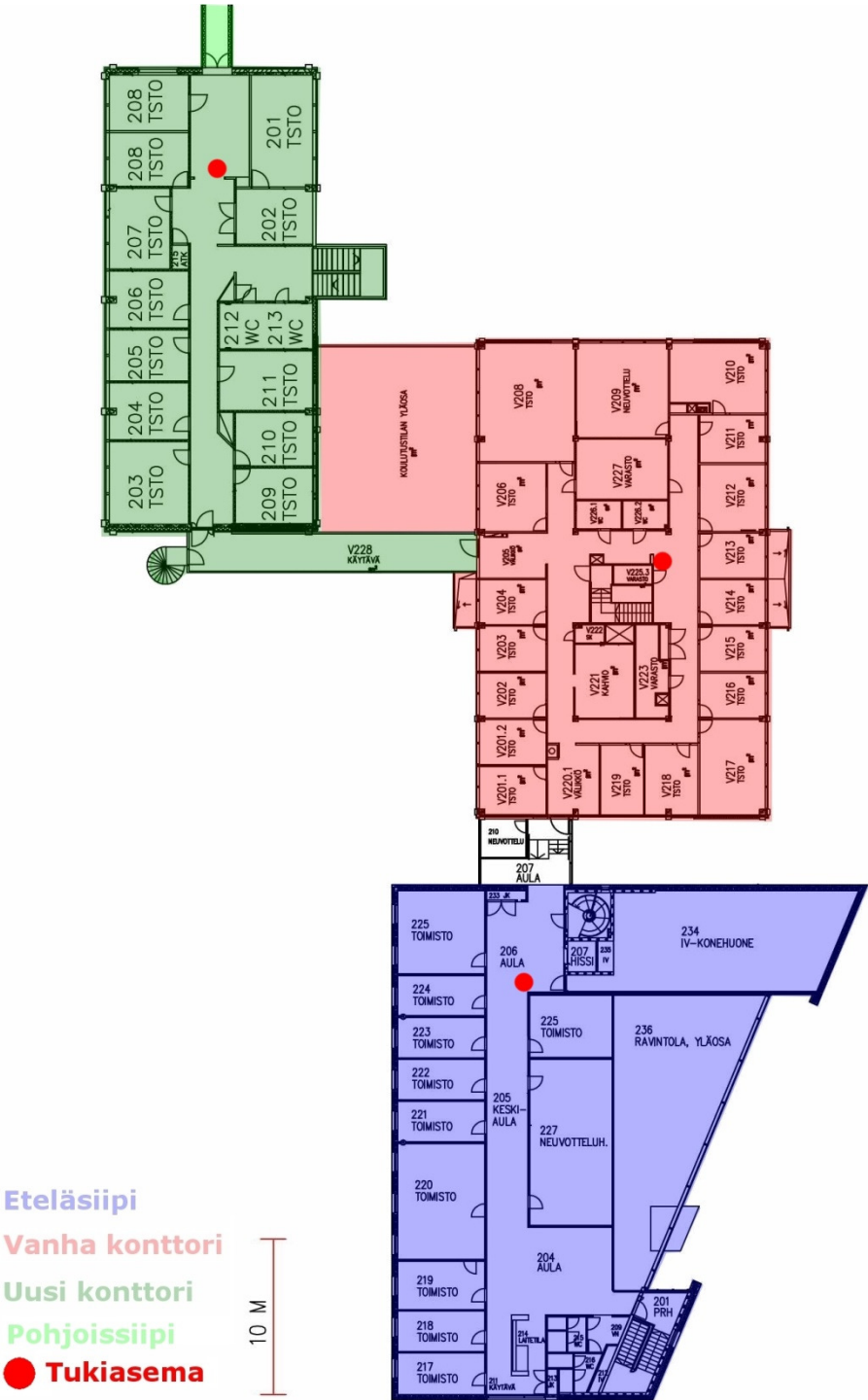
Pohjakuva:

- Pohjakuvissa pääkonttori on jaettu osiin: Eteläsiipi 1-3. Krs., Vanha konttori 1-2. Krs., Uusi konttori 1-2 Krs., Pohjoissiipi 2. Krs.
- Kuvista käy myös ilmi tukiasemien 9kpl suunnitellut sijainnit.

1. Kerros

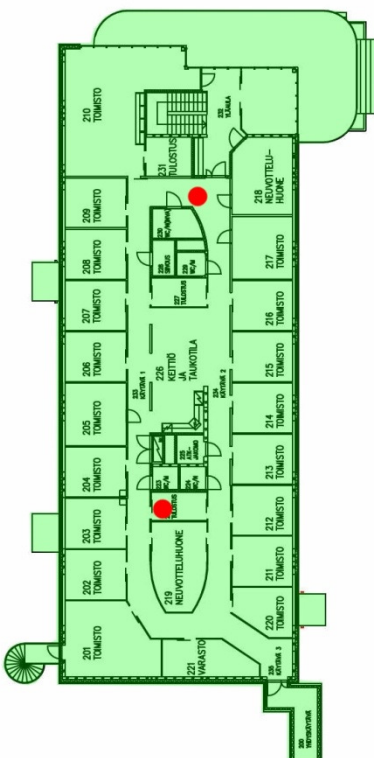


2. Kerros





10 M



3. Kerros

